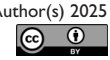
Original Article

EJIR

European Journal of International Relations
1–38



DOI: 10.1177/13540661251382639
journals.sagepub.com/home/ejt
Sage

Resisting disinformation: theorising whole-of-society and sociotechnical resistance

Mariah Thornton
The London School of Economics and Political Science (LSE), UK

Abstract

How can states resist transnational disinformation campaigns? Analyses in the field of International Relations (IR) have offered a variety of explanations which index the harms of disinformation to state power, yet state resistance to disinformation remains underexplored and under-theorised. Through the concept of a 'mobilisation of resistance' and based insights from Social Theory and Science and Technology Studies (STS), this article posits a social-processual framework to explain whole-of-society resistance to transnational disinformation and the role of sociotechnical systems in facilitating this resistance. This approach emphasises the agency of civil society actors and sociotechnical systems in articulating resistance to transnational disinformation alongside the state. The article specifies four processes through which a mobilisation of resistance to disinformation can be expressed through technology: enframing, co-production, legitimation and humour. As a country at the forefront of combatting disinformation from China, Taiwan presents a valuable empirical site through which resistance to transnational disinformation can be understood. Taking Taiwan's open-source governance (OSG) and algorithmic co-governance (ACG) as paradigmatic cases of whole-of-society sociotechnical resistance, I seek to illustrate how these four processes have been materially enacted to resist Chinese disinformation campaigns on the one hand while promoting a democratic social order in Taiwan on the other hand.

Keywords

Disinformation, whole-of-society resistance, sociotechnical resistance, open-source governance, algorithmic co-governance, Taiwan, China, cross-Strait relations

Corresponding author:
Mariah Thornton, The London School of Economics and Political Science (LSE), Houghton Street, London WC2A 2AE, UK.
Emails: m.thornton1@lse.ac.uk; mariaht.thornton@gmail.com

Introduction

The potential of disinformation to influence a population's emotions and beliefs towards political elites, institutions and processes has remained an enduring threat to democracies the world over and became a recurring theme over the 2024 super-election year. Advances in generative artificial intelligence to rapidly and seamlessly produce disinformation narratives as well as generate 'deep fakes' has compounded these challenges. International Relations (IR) has offered a wealth of explanations on how transnational disinformation campaigns impact state power while also debating the severity of their effects (Anzera and Massa, 2021; Bolton, 2020; Farrell and Newman, 2021; la Cour, 2020; Lanoszka, 2019; Manfredi et al., 2022; Maschmeyer, 2023; Wohlforth, 2020). Though scholars have begun to explore how states can deter disinformation (Hedling and Ördén, 2025), theories and empirical cases of state *resistance* to disinformation remain largely underexplored and underdeveloped in the field. Similarly, while discussions of 'whole-of-society resistance' against disinformation campaigns are prevalent in the policy world (Helmus and Holynska, 2024; Maddox et al., 2021; NATO Parliamentary Assembly, 2021; Niinistö, 2024; Wigell, 2021), there is a lack of theoretical engagement with this phenomenon in IR.

This is due in part to the IR disinformation literature's fixation on the state and less so on other actors that come into contact with disinformation campaigns, including the societies that are targeted by disinformation as well as the sociotechnical systems involved in transmitting and identifying it. As actors now have unfettered agency in the dissemination of information due to the rise of social media, disinformation scholars must treat the realm of public diplomacy as no longer limited to the state (Manfredi et al., 2022: 208). In this vein, to explain whole-of-society resistance and ultimately state resistance against transnational disinformation campaigns, the agentic capacities of civil society actors and social technologies must be accounted for. Simply put, theories which account for the 'society' dimension in whole-of-society resistance are required. Whole-of-society resistance can be understood as collaboration between the state and civil society actors to counter external interference, in contrast to states relying exclusively on military or diplomatic efforts (Maddox et al., 2021; Wigell, 2021). Social Theory and the related field of Science and Technology Studies (STS) can articulate a framework for whole-of-society and sociotechnical resistance to transnational disinformation by offering insights into the relationship between societies, technologies, resistance and state power. As technologies have become increasingly enmeshed in networks of global power, STS has not only strived to explain sociotechnical systems' role in reproducing structures of power but also how they are utilised in resistance to them (Pollock and Subramaniam, 2016: 952). These interventions stand to enrich the IR disinformation literature by furnishing theoretical explanations of whole-of-society and sociotechnical resistance against transnational disinformation which stress the agencies of social actors and social technologies.

The core question of this article is: *How can states and their societies enact whole-of-society resistance to transnational disinformation campaigns through sociotechnical systems?*[1] Drawing from the fundamental view held in Social Theory and STS that technologies are producers of social order, this article explores how sociotechnical systems contribute to constructing social orders that can resist disinformation and strengthen

public trust in governance. This article leverages Social Theory and STS to emphasise the salience and interconnected agencies of civil society actors as well as technologies in resisting disinformation alongside the state. This represents a departure from the state-centric theoretical explanations of disinformation which dominate the field of IR, paving the way for deeper engagement with the role of civil society actors and sociotechnical systems in studies of transnational disinformation as well as greater attentiveness to the social, political and historical contexts which inform responses to it. STS also allows us to consider how technologies can shape perceptions of a state and its governance in ways that reinforce social order, potentially serving as an antidote to the outrage and mistrust that disinformation campaigns often seek to inspire against it. This contrasts with the prevailing view of sociotechnical systems in the IR disinformation literature as disruptors of state power and furthermore empowers the field to examine the positive bearing of sociotechnical systems on governance and society-wide support for the state. Social Theory and STS therefore offer a starting point in theorising whole-of-society and sociotechnical resistance to transnational disinformation campaigns.

Taiwanese resistance to Chinese disinformation presents an ideal case to demonstrate this theoretical contribution. As a democracy that has been inundated with disinformation campaigns from China, and as a state with a highly technologically literate and dynamic civil society engaged in resistance to Chinese disinformation, Taiwan presents valuable empirical evidence to answer the question of how states and their societies can resist disinformation with the support of sociotechnical systems. Taking Taiwanese resistance through open-source governance (OSG) and algorithmic co-governance (ACG) technologies as its focus, this article investigates how the case of Taiwan resonates with other cases of whole-of-society and sociotechnical resistance to disinformation. On a theoretical level, Social Theory and STS are deployed to theorise whole-of-society resistance to transnational disinformation through technology. This framework is then applied to investigate how Taiwan's OSG and ACG sociotechnical systems resist China's disinformation campaigns and bolster trust in the Taiwanese state.

This article has four overarching goals. First, to outline a theoretical framework for understanding resistance to transnational disinformation which scholars of IR and International Studies can utilise to further develop explanations of democratic whole-of-society resistance that may resonate with other cases beyond Taiwan. Second and related, to offer an analytical approach which restores the agency of societies and technologies in resisting disinformation alongside the state, a perspective which can foster constructive engagement between the IR disinformation literature, the policy world, as well as Social Theory and STS. Third, to positively illustrate how democratic states can work with their civil societies and utilise sociotechnical systems to resist transnational disinformation campaigns and increase public trust in governance. Fourth, to draw attention to empirical insights from Taiwanese sociotechnical resistance to Chinese disinformation, thereby contributing a non-Western case study to a burgeoning academic literature on resisting and deterring disinformation (Hedling and Ördén, 2025; Lahmann, 2022; Monsees, 2023; Pherson et al., 2021; Wigell, 2021; Wilner, 2024).

This article begins by taking inventory of the existing literature on disinformation and state power in IR. It then expounds a theoretical framework based on a social-processual approach to disinformation and resistance. Within this framework, I operationalise the

concept of a 'mobilisation of bias' – forms of political organisation in which certain topics and actors are *organised in* and *organised out* of the decision-making process (Schattschneider, 1975: 71) – to explain whole-of-society resistance to transnational disinformation. I describe this phenomenon as the 'mobilisation of resistance'. While the mobilisation of bias describes how power is exercised through agenda-setting, the mobilisation of resistance demonstrates how this agenda-setting can be structured to *resist* or exclude certain discourses, topics and actors, including disinformation. Taking the mobilisation of bias as a site of resistance, I then leverage Social Theory and STS to highlight four distinct processes through which state-society resistance to disinformation can be facilitated through sociotechnical systems: (1) enframing, (2) co-production, (3) legitimation and (4) humour. Finally, I illustrate how these four processes are materially enacted through Taiwan's OSG and ACG sociotechnical systems.

State power and disinformation in IR

Disinformation is composed of discourses and images which contain 'misleading information that [has] the function of misleading' (Fallis, 2015; Lanoszka, 2019). Based on Lukes's (1974) power framework, disinformation represents a latent form of power that cannot be contained within defined physical borders – where successful, it can influence individuals' perceptions of their own wants and needs, and potentially spread throughout communities in ways that subvert a state's capacity to exercise its power. The tendency of disinformation to deploy misleading discourses and images to disrupt state power has led to its conceptual confusion with misinformation and other tools of statecraft such as narratives and propaganda. To clarify, misinformation lacks disinformation's intent to mislead, it is *accidentally* incorrect (Lanoszka, 2019; Lewandowsky et al., 2013: 488). Moreover, though disinformation and misinformation have been compared to propaganda and narratives, the difference lies in disinformation's fundamental intention and function to mislead with false information. Unlike disinformation, the actors creating narratives and propaganda do not necessarily know their content to be false (la Cour, 2020). Disinformation also seeks to dismantle shared values by enflaming mistrust whereas narratives aim to build a sense of collective identity or understanding of an event (la Cour, 2020).

International Studies has illuminated the many dimensions through which disinformation campaigns challenge the power of governing elites, including the destabilisation of norms through deception (Farrell and Newman, 2021; Lanoszka, 2019), subversion of state structural power (Maschmeyer, 2023; Wohlforth, 2020), disruption to a state's ability to stabilise its identity through narratives (Bolton, 2020; Lupovici, 2023), as well as the capacity of disinformation narratives to influence target populations at an ideological, emotional and spiritual level (la Cour, 2020). Disinformation campaigns represent a systematic government effort aimed at using disinformation to mislead a particular audience to influence the policy process (Lanoszka, 2019). When wielded in inter-state conflicts, disinformation campaigns can damage state power by warping public perceptions of the state, its representatives and its governance, potentially causing social unrest. The efficacy of disinformation campaigns therefore hinges upon altering the ways in which a state is imagined in the minds of target communities across a society. Two theoretical

explanations within the IR disinformation literature have emerged to specify the nature of these harms: ontological security (OS) and subversion.

OS has observed the potential of discourses amplified by cyber technologies to undermine the state's status as an ontological security provider for its citizens, hampering its ability to maintain coherent narratives, routines and a sense of home (Lupovici, 2023). Transnational disinformation campaigns serve as an example of how states use social media platforms to advance information warfare that undermine other states' endogenous sources of ontological security (Bolton, 2020). By targeting the bonds of society, disinformation impacts the communities from which a state's 'ordering of the environment' is derived, thereby damaging citizens' ability to stabilise their sense of self vis-à-vis the state (Bolton, 2020). Disinformation achieves this by arousing public scepticism towards the 'national subjectivity' – how individuals understand themselves in relation to the state – thereby producing anxiety and crisis to erode 'the Self' (Bolton, 2020). Based on this understanding, the OS and cyber literatures have tended to characterise technologies as threats to state power and security (Choucri and Clark, 2019 [2018]; Dunn Cavelty, 2010, 2015; Green, 2015; Lambach, 2020; Lupovici, 2023).

Alongside OS explanations, subversion has also been utilised to explain disinformation's adverse effects on state power. Drawing from realism, subversion has been described as a form of statecraft in which a state pursues strategic action against a target state to influence its domestic political environment in service of certain foreign policy goals (Wohlforth, 2020: 461). Subversion has two defining characteristics. In contrast to altering the external environment to induce change in state behaviour, subversion directly affects the domestic processes within a territory and contradicts the target state's interests (Wohlforth, 2020: 461). Building on this conceptualisation, subversion through disinformation has been theorised as the exploitation of a state's structural power, or its ability to shape structures of interaction and the capacities of structural positions (Barnett and Duvall, 2005; Maschmeyer, 2023). Subversion reverse-engineers the benefits of structural power into harms to the state by exploiting vulnerabilities in structures to manipulate them as well as produce unexpected and unintended outcomes (Maschmeyer, 2023). Akin to the OS literature, the subversion literature predominately views technology as tools that advance subversion statecraft, for example by taking advantage of a state's open information systems to harvest data which is then used in disinformation campaigns against those states (Maschmeyer, 2021, 2023). This perspective similarly implies technologies only exacerbate the threat of subversion to the state, and are ultimately injurious to its sovereignty and structural power.

While both literatures have provided valuable theoretical lenses through which scholars can index the harms of transnational disinformation to the state, the IR disinformation literature currently suffers from two limitations. First, it gives primacy to the analytical unit of the state and in so doing treats societies as well as digital platforms and technologies as passive sites through which disinformation campaigns are merely transmitted to subvert state power. In narrowing its focus on the state and statecraft, the realm of domestic politics and society is implicitly relegated to the subordinate position of being a source of state power. As such, the specific social actors, institutions and processes which actively construct and maintain state power in the face of threats like disinformation remain largely unaccounted for. Such a perspective therefore overlooks and often omits

the agency of civil society actors and social technologies in enabling or constraining the impact, spread and duration of transnational disinformation. This prevents the literature from meaningfully addressing the question 'Why is transnational disinformation more impactful in this context yet met with resistance in another?' Second, both the OS and subversion literatures tend to characterise technologies simply as tools used by actors to damage state power. This is because technologies are seen as magnifying disruption and uncertainty when it comes to governance. However, this view fails to critically engage with the role technologies so often play in safeguarding, maintaining and reproducing state power as well as bolstering state resilience to withstand the challenges of subversion and disinformation. Taken as a whole, the IR disinformation literature therefore neglects the active and positive roles social actors and sociotechnical systems can play in resisting disinformation as well as in building a constructive relationship between civil society and the state. Only by refocusing on the agency of societies and technologies in relation to the state can their capacity to not only transmit but also *resist* disinformation be theoretically examined.

Social Theory and Science and Technology Studies (STS) can address the limitations within the IR disinformation literature with two key interventions. First, by relocating the agentic capacities of both society and technology in the (re)production of social order and by extension state power. Second, by providing insight into the specific processes through which these agentic capacities inform whole-of-society resistance to transnational disinformation. Based on these interventions, the next section outlines a social-processual framework to explain whole-of-society resistance to transnational disinformation campaigns. Drawing from Social Theory and STS, the framework stresses the agency of sociotechnical systems in (re)producing social orders which govern the individual and society, and how these relate to state power. The concept of the 'mobilisation of bias' is operationalised to explain whole-of-society resistance to transnational disinformation campaigns, a phenomenon which I term the 'mobilisation of resistance'. Building on the idea of the mobilisation of bias as a site of resistance, I expound four specific processes that contribute to a 'mobilisation of resistance' against disinformation – enframing, co-production, legitimation and humour – and explore the role sociotechnical systems play in facilitating these processes.

Society, technology and resistance: towards a social-processual framework

The field of journalism and communication studies has stressed the salience of relational approaches and social factors in explaining the impact of disinformation as well as processes through which its impact can be minimised (Dodds, 2021; Garusi and Leonhardt, 2024; Lindquist and Weltevrede, 2024; Waisbord, 2018). Yet none have explicitly applied social processualism as a theoretical framework to resistance against disinformation. Processualism examines the conditions under which social structures emerge and stabilise (Abbott, 2016: 3, 23–24). A processual ontology treats phenomena in social and political life as lineages in which 'various events are linked together, nonexclusively' (Abbott, 2016: 24). These lineages are reproduced at the micro, personal level as well as

at the macro, societal level. A social-processual approach to the transmission of disinformation and resistance to disinformation would involve treating both as occurring within a lineage and examining the historical, cultural and political context through which either recurring transmission of disinformation or resistance to disinformation might unfold. This approach would also scrutinise the extent to which disinformation campaigns impact the social orders they seek to disrupt, exploring whether they led to change or continuity in existing structures, as well as examining the social conditions which shaped that outcome. Finally, a social-processual framework to disinformation would not demarcate between the individual and social groups 'since both are simply lineages defined on events' (Abbott, 2016: 24, 75).[2] A social-processual approach would therefore extend its analysis beyond the agency of the state – itself an 'ecology' of different groups (Abbott, 2016: 36) – by examining the agency of 'immense social forces' in shaping outcomes (Abbott, 2016: 5, 13, 15), including those relating to disinformation.

As civil societies are the primary site upon which transnational disinformation campaigns are enacted and resisted, a social-processual lens stands to benefit the IR disinformation literature in several ways. First, it offers a framework for understanding disinformation in a less state-centric way by spotlighting the agency of civil society in shaping certain outcomes, whether that be a population's transmission of disinformation narratives or resistance against them. This in turn paves the way for developing theoretical explanations of whole-of-society resistance against disinformation. Second, it provides an approach through which scholars can index the social, historical and cultural factors that may explain why transnational disinformation campaigns are effective in certain contexts and not in others. This represents a departure from ontological security analyses of disinformation within IR which fixate on the agency of the state as the provider of ontological security, while 'social forces' and the agency of civil society actors tend to be amalgamated and subsumed under the state. By contrast, a social-processual approach accords more equal weighting to the agency of individuals and civil society actors vis-à-vis the state as well as highlights the interconnections between these agencies in (re)producing outcomes of social-political importance, such as whole-of-society resistance to disinformation.

The first step in developing a social-processual framework would be to consider the social conditions under which transnational disinformation campaigns are impactful. Disinformation is a type of information (Fallis, 2015), and information itself is a communicative construct produced in a social context (Karlova and Fisher, 2013; Tuominen and Savolainen, 1997). The transmission of disinformation is a social act through which misleading information is used by individuals to collectively construct a shared reality (Karlova and Fisher, 2013). When disinformation goes 'viral', this shared reality expands and bears on the perceptions of communities, thereby transcending the individual and potentially mobilising society in ways which affect political decision-making processes, and by extension the state. For example, the insurrection of Capitol Hill on 6 January 2021 saw thousands of Trump supporters commit acts of political violence based on false narratives that the US presidential election was 'stolen'. This raises the question: *What motivates the transmission of disinformation in the first place*? Uncertainty, importance, or outcome-relevant involvement, lack of control, anxiety and belief are all factors which have been identified as informing the individual's choice to pass on unverified

information to others (Wang, 2020). Rumour transmission is a 'human social behaviour goal' aimed at acting effectively, building and maintaining relationships, and managing favourable self-impressions (Wang, 2020: 71). Individual anxiety can arise from feelings of uncertainty over issues of personal importance, which can cause people to engage in fact-finding (Wang, 2020: 72). Individuals therefore often turn to informal social networks to obtain information and reduce their anxiety (Wang, 2020: 72). The social and affective motivations behind the spread of disinformation are therefore clearly intertwined and transcend the individual to span entire communities in ways that can affect governance, social order, and by extension the state.

Science and Technology Studies (STS) has long observed the capacity of technologies to (re)produce social orders. It is therefore well-positioned to provide insights on the relationships between sociotechnical systems, the individual and society in constructing – rather than eroding – state power. STS offers three relevant insights on this point. First, STS treats technology as enmeshed with society and as integral components of social order (Jasanoff and Kim, 2015: 2). Human choice and preference inform the design of technologies, the ways in which they organise information, their calculations of risks and benefits which we rely upon to inform our decision-making, and the human behaviours they promote, exclude and regulate (Callon, 1987 (1986); Jasanoff, 2006; Jasanoff and Kim, 2015). The pervasiveness of social media and smart phones in social life demonstrates technologies play a central part in structuring the systems of knowledge and information which inform broader social orders. Technologies are therefore not neutral intermediaries between humans and the physical world, but rather directly shape 'what it is to be human in the world' and as such are endowed with agentic capacity (Hoijtink and Leese, 2019; Matthewman, 2011: 13). This insight can enrich the IR disinformation literature by allowing greater exploration of the agency of the technologies involved in generating and spreading disinformation as well as those resisting it, and how this agency interacts with the social order it encounters. In other words, STS explores technology's capacity to (re)produce social-political orders that affect states and their governance, which may in turn affect the power dynamics between states on a global scale. At a methodological level, STS therefore links the local and everyday uses of technologies with broader trans-geographic and trans-temporal systems (Kleinman and Moore, 2014: 5). Second and related, STS seeks to explain how human development and use of technology is intimately connected to how individuals and societies govern themselves. This perspective stresses the agency of technology in influencing how individuals perceive the 'real world' (Jasanoff and Kim, 2015: 3). Technology therefore has agency and power in impacting users' perceptions by governing their modes of interaction as well as influencing what they imagine their needs and wants to be. This may in turn affect a state's governance of its society in response to those perceived needs and wants, something which disinformation campaigns seek to distort and exploit for strategic ends. Third, STS posits that while technologies have agency in influencing social orders, they are at the same time shaped by the social orders within which they are created (Jacobsen and Monsees, 2019; Jasanoff, 2004). Sociotechnical systems can therefore not only structure but also be structured by states and civil society actors to promote and reinforce certain values, ideas and discourses while excluding others, such as disinformation.

By adopting an STS approach, we can understand that societies and technologies not only have agency in (re)producing social orders, but that these agencies are co-constitutive. On the one hand, applications of technology to the 'real world' are socially conditioned, and on the other hand, technologies reflect and reinforce the social orders within which they exist. Technologies therefore not only have the capacity to challenge state power but often actively construct it by regulating certain behaviour, organising information, as well as advancing specific discourses, values and practices. Applying this to the phenomenon of disinformation, the societies and social technologies targeted by disinformation are not merely influenced by it; they also have the potential to exercise agency by resisting disinformation in favour of preserving the social order. It is well known that state-sponsored disinformation campaigns exploit the open information environments of democratic states to advance anti-democratic narratives among the public. Democracies can therefore counter these activities by collaborating with the societies they govern to consolidate a democratic order with the aid of technology. This represents a kind of whole-of-society resistance to disinformation, one in which civil society actors and sociotechnical systems can play an active role. Due to its emphasis on the capacity of technologies to produce social orders, STS presents a framework for understanding how sociotechnical systems can construct orders which resist transnational disinformation.

This begs the question: *How might states, societies and sociotechnical systems materially enact resistance to transnational disinformation campaigns*? Resistance can be understood as the way in which the relationships of power are altered (Gaventa, 1980: 4). Resistance develops where there is a shift in power relationships, either owing to A's loss in power or B's gain in power (Gaventa, 1980: 22). Disinformation can subvert a state's structural power – its ability to shape structures of interaction and the capacities of structural positions (Barnett and Duvall, 2005; Maschmeyer, 2023) – by inspiring mistrust among communities towards political elites, institutions and processes. Disinformation is therefore a tool of ideational power as it has the potential to shape the perceptions of others.[3] Disinformation campaigns, where successful, can inspire social conflict by distorting a community's perception of the state, its officials and governance. Based on Gaventa's framework, effective resistance to transnational disinformation would entail either diminishing the ideational power of A's disinformation narratives against B or strengthening B's ideational power at the expense of A's disinformation narratives. Since foreign publics are so often the target of disinformation, mitigating disinformation campaigns' potential to exercise ideational power requires enlisting the resistance of civil society actors.

Whole-of-society resistance against transnational disinformation can be understood through the concept of a 'mobilisation of bias'. The mobilisation of bias represents the sites through which structural power is (re)produced between elites and those governed by elites, specifically forms political organisation that 'have a bias in favour of the exploitation of some kinds of conflict and the suppression of others'. Simply put, the mobilisation of bias refers to the ways certain ideas and actors are *organised into* politics while others are *organised out* (Schattschneider, 1975: 71). The mobilisation of bias explains how institutions and social practices structure decision-making within politics, accounting for the role of agenda-setting and non-decision-making in exercises of power (Bachrach and Baratz, 1962: 948; Guzzini, 1993; Lukes, 1974). Schattschneider (1875:

76–78) originally developed the mobilisation of bias to explain how the US Republicans weaponised factionalism in the Democratic Party caused by the 1896 Populist movement to consolidate their power in ways that shaped the dominant political agenda for three decades. This contributed to a mobilisation of bias which *organised in* a pro-elite, pro-business agenda into American politics, thereby strengthening the power of the Republican party system while also *organising out* non-elite, working class political agendas. Gaventa (1980: 78) similarly described a mobilisation of bias present within Middlesboro Tennessee which continually reinforced the power of industry elites who exploited the region's natural resources while quashing any local resistance to the glaring socioeconomic inequality this exploitation caused. Given the prevalence of technologies in social life, sociotechnical systems are integral to agenda-setting within a mobilisation of bias. Though not explicitly linked to the mobilisation of bias, studies within STS stress the bearing of science and technology on agenda-setting not only by generating structures of knowledge but also structures of 'non-knowledge' (Frickel, 2014: 267). Overall, the mobilisation of bias therefore organises the sites of conflict and resistance prevalent in social-political life, often with the support of sociotechnical systems. The mobilisation of bias thus stresses the institutions, cultures and discourses through which agenda-setting is enacted, while STS explains how technologies support this agenda-setting.

Though the mobilisation of bias has frequently been deployed to illustrate cases of undemocratic domination, I refashion the concept as a way of explaining whole-of-society resistance to disinformation campaigns, or what I term a 'mobilisation of resistance', and how this can be applied to democracies. This is based on the understanding that agenda-setting within a mobilisation of bias is not always simply a tool to exert domination. Agenda-setting can also centre on enhancing participatory democracy and resisting subversion activities which seek to undermine democratic systems, a phenomenon which I believe the case of Taiwanese resistance to Chinese disinformation highlights well. If one understands resistance as changing the relationships of power (Gaventa, 1980), a mobilisation of bias can change state A's use of disinformation to subvert state B's structural power through disinformation by *organising in* certain ideas and practices, such as fact-checking and public trust in state representatives and political processes, as well as *organising out* narratives commonly advanced by disinformation campaigns such as elites' inability to govern or callous disregard for citizens' wellbeing. By setting agendas which promote trust in democratic political systems on the one hand and mitigate the impact of disinformation through fact-checking or digital literacy education on the other hand, democracies can establish a mobilisation of resistance, thereby fostering whole-of-society resistance to disinformation. For example, in response to Russian disinformation campaigns which fuelled violent protests in Tallin, Estonia made media literacy a part of the national curriculum from kindergarten to high school, requiring students in the 10th grade to partake in a 'media and influence' course (Yee, 2022). Estonia ranked fourth out of 41 countries in the European Media Literacy Index 2023, indicating strong potential to withstand disinformation (Lessenski, 2023). Estonian countermeasures against Russian disinformation therefore involved establishing a mobilisation of resistance which *organised out* the potential for social conflict sparked by fake news through media literacy education. The mobilisation of bias is therefore not only a site of power but also resistance because it can be structured to attenuate disinformation's influence on societies and by extension states.

The mobilisation of bias also shows society has agency in impacting state power in two ways. On the one hand, society has the capacity to reinforce a mobilisation of bias through offering its latent 'consent' in the form of trust in governing elites and their associated ideologies. On the other hand, society also has the capacity to resist governing elites through a 'mobilisation of action' by developing consciousness of the needs, possibilities and strategies of resistance to overthrow the incumbent mobilisation of bias (Gaventa, 1980: 24, 71). Disinformation campaigns may seek to subvert a state's mobilisation of bias by causing public mistrust and suspicion, potentially instigating a mobilisation of action against the state. However, I argue that society and sociotechnical systems can collaborate with the state by contributing to a mobilisation of resistance against transnational disinformation campaigns which *organises out* misleading discourses that inspire mistrust towards democracy while *organising in* trust towards the democratic state. Building on this, I draw on the fundamental insight of STS – that technologies are producers of social order – to make the case that sociotechnical systems have agency alongside society in forging a mobilisation of resistance and a democratic social order, thereby contributing to a state's whole-of-society resistance to disinformation.

While the mobilisation of bias offers a way of conceptualising whole-of-society resistance to disinformation campaigns, Social Theory and STS can be leveraged to further develop a processual framework for understanding the specific *processes* through which this resistance can be implemented by civil society actors and sociotechnical systems. Both fields highlight four processes which I argue are pertinent to explaining Taiwanese resistance to Chinese disinformation campaigns through open-source governance (OSG) and algorithmic co-governance (ACG) sociotechnical systems: (1) enframing, (2) co-production, (3) legitimation and (4) humour. As with any process which constructs social order, all four processes harbour an inherent duality: they can be utilised to advance undemocratic forms of domination and hegemony, but they also have the potential to advance democratic social orders, the latter of which is the focus of this article.

Enframing

The essence of technology is enframing (*ge-stell*), which involves '[driving] out every other possibility of revealing' (Heidegger, 2013). Revealing concerns uncovering the true nature and essence of objects and phenomena in the world (Blitz, 2014: 69). Technology is itself a way of revealing – its true essence lies in demonstrating the way in which all entities, not just machines and technical processes, present themselves (Blitz, 2014: 69). In an instrumental sense, technologies take a complex natural object or phenomenon and simplify it into a set of components that the user of the technology can order, conscript, assemble, or disassemble (Blitz, 2014; Heidegger, 2013: 68). Enframing refers to a process by which humans 'order' a natural object or phenomenon into a resource to be used – what Heidegger referred to as 'standing reserve' – and convert this standing reserve into a larger system of utility (Ruin, 2009: 191). Enframing makes this conversion appear seamless and natural to the users of the technology. In so doing, enframing excludes other possible interpretations, uses and understandings of the true essence of the object or phenomenon that is being converted. As such, enframing often

obscures the *ontology* of a technology, yet superimposes that ontology in material ways (Harman, 2010: 17). For example, technologies like hydroelectric works harness and convert a natural resource such as a flowing river to produce electricity, thereby organising it into electricity supply at the same time as naturalising the idea of electricity as a resource to be harvested and consumed. Enframing obscures other ways flowing water may be conceptualised. Through the process of enframing, technologies like hydroelectric works therefore facilitate how human beings understand, order and present natural phenomena to themselves (Ruin, 2009: 192). Enframing is therefore a process which impacts the ordering of structures of knowledge and consumption which in turn shape human behaviour, core concerns of STS. Enframing has informed explanations of these phenomena in STS. For example, Borgmann's (1984: 80–81) device paradigm draws on enframing to illustrate how modern technologies condition our modes of engagement with the world as well as temper how we ascribe value to experiences. Enframing has also been used within the STS literature to explain how corporate information networks construct and manage customer experiences (Ciborra, 2004: 55–82).[4]

Following from the STS literature on enframing, I argue enframing can involve ordering discourses and information into a system of understanding that is consumed by individuals. Technologies that enframe information and discourses therefore have a profound impact on how users perceive 'truth' and interpret phenomena around them. This eliminates other possible interpretations of information and discourses, or other modes of 'revealing'. When a technology is prevalent in social life, such as social media, enframing can occur when information and issues are *organised into* and *organised out* of society through algorithms. Enframing through algorithms can thus affect agenda-setting, and therefore a state's mobilisation of bias. Enframing systematises and naturalises how people interpret information online, including disinformation, while excluding other possible interpretations of that information. Enframing is therefore one of the processes through which a mobilisation of resistance to disinformation can be facilitated at a socio-technical level.

Fact-checking platforms such as Snopes and PolitiFact's Truth-O-Meter can be considered cases of resistance through enframing. This is because these interfaces convert discourses in the form of rumours, 'fake news', or claims by made by political representatives and present them as a succinct evaluation based on fact-checking criteria. This conversion is organised into a wider system of utility, such as a search engine in the case of Snopes or a ranking system, news site, and social media platform in the case of PolitiFact. The result of this systematised fact-checking through technology is that it drives out other possible interpretations of the information to its users. In this way, Snopes and PolitiFact arguably *enframe* resistance to dis/misinformation by structuring technological interfaces to naturalise fact-checking. If used widely, enframing through these technologies may contribute to a mobilisation of resistance against disinformation by organising out misleading discourses and 'fake news'.

Co-production

Co-production refers to 'the ways in which we know and represent the world (both nature and society) are inseparable from the ways in which we choose to live in it' (Jasanoff,

2004: 2). Though originally described as an 'idiom', co-production has been used as an analytical perspective to explore how actors organise and express themselves, assign value to ideas as well as physical things, and assume responsibility for their inventions through the organisation of knowledge and technology (Jasanoff, 2004: 6). As an analytical approach, co-production links the micro-level organisation of information through technology to the macro-processes which generate social order (Jasanoff, 2004: 28). However, co-production can also be understood as a *process* in two ways. First, co-production involves the social production *of* technology, or how a social order shapes a technology as well as its uses and 'real world' implementation. Second, co-production also encapsulates social production *by* technology, or how technologies themselves generate, maintain and (re)produce social orders (Jacobsen and Monsees, 2019: 27). Co-production therefore examines the processes through which the world is ordered by social actors and technologies (Jasanoff, 2005: 23). Compared to enframing, co-production centres more on explaining the ways in which technology simultaneously reflects and (re)produces certain social orders; it intertwines the agency of social actors and technologies. Enframing on the other hand focuses on the agency of technology in ordering and converting natural resources into a wider system of consumption, representing only one aspect of co-production.

Though co-production has spotlighted the ways in which states instrumentalise discourses about technology to expand their power (Jasanoff, 2005: 23), I argue co-production can also be a sociotechnical process through which the relationships of structural power between a democratic state and the society it governs can be positively reinforced. This is because co-production accords agency to society in the way it orders technologies and their uses while at the same time accounting for technology's agency in reinforcing certain values, practices and orders by extension. In this way, co-production lends explanatory power to the *organising in* aspect of a mobilisation of bias by showing how agenda-setting is facilitated through technology. For example, by promoting the use of biometrics in processing refugees as 'safe', 'tested' and 'trusted', the United Nations High Commissioner for Refugees (UNHCR) arguably produced a social order in which the harvesting of refugees' personal data through biometrics technology was normalised across other international development agencies (Jacobsen and Monsees, 2019: 27). In this way, the UNHCR contributed to a mobilisation of bias which promoted the registration and tracking of refugees, while the biometrics technology itself reinforced an order in which these practices were systematised and standardised on a global level. Co-production can reinforce oppressive power structures as the UNHRC example suggests, but it also has the potential to promote those that are democratic, as this article will explore in the case of Taiwan.

In this vein, co-production represents another sociotechnical process that can facilitate a mobilisation of resistance to disinformation. Numerous transnational disinformation campaigns have sought to erode public trust in democracy's ability to meet their needs. Democratic states and societies can therefore resist disinformation by structuring sociotechnical systems to *organise in* trust towards political representatives and processes. In so doing, democracies can reinforce a pro-democratic social order in which a certain degree of public trust in its representatives and governance is fundamental, thus

mitigating the potential of anti-democratic disinformation narratives to ignite widespread social unrest. For example, Estonia's nationwide digitalisation of state services through e-Estonia represents a case of co-production which arguably contributed to the country's resistance against Russian disinformation campaigns. The development of e-governance in Estonia was based on the 1998 Principles of Estonian Information Policy which supported the government's digital transformation to increase the efficacy of its governance and delivery of public services (OECD, 2019: 208). A crucial step within this digital transformation was the creation of mandatory e-cards for citizens. Today, 99 percent of public services are available to citizens via E-Estonia 24 hours a day, such as Internet voting (i-Voting), public consultation in the drafting of laws through Eelnõude infosüsteem (EIS), and digital record-keeping of healthcare through e-Health record (e-Estonia, 2024). On the one hand, the technology of e-cards facilitated a social order in which individual data security and transparency were fundamental to the government's delivery of public services. It must be observed this led to greater state control over the collection and maintenance of individuals' data. This represents the social production *by* technology. On the other hand, e-cards were also promoted by the state as a way of maximising the efficiency and accessibility public services. It is claimed that 82 percent of citizens trust the government's e services (e-Estonia, 2024). This represents the social production *of* technology, as the Estonian government promotes e-Estonia as an effective and trustworthy platform for Estonian democracy (Kingsley, 2012). It has been argued that e-Estonia fostered a kind of digital sovereignty that consolidated Estonia's position as a progressive democracy and distanced itself from its Soviet past (Budnitsky, 2022). Alongside other initiatives such as digital literacy education, e-Estonia arguably consolidated resistance against Russian disinformation narratives by bolstering public trust in government services. E-Estonia therefore co-produced a democratic order by *organising in* trust for Estonian officials and institutions across state-society relations through its digital interfaces. Co-production is therefore a process through which a mobilisation of resistance to disinformation may be facilitated through technology, its users and governing elites.

Legitimation

The process of legitimation is closely linked to the *social production by technology* element within co-production. However, unlike co-production, legitimation better accounts for the affective dimensions of *organising in* the trust of individuals and society towards the state. In short, legitimation explains the emotions involved when trust is conferred from one actor to another, whereas co-production stresses how the structuring of technologies and the discourses relating to them shape and (re)produce social orders. Co-production emphasises the agency of the technology as well as the users of the technology, whereas legitimation specifically captures how the agency of those being governed is exercised towards governing elites and the affective dynamics of this relationship. Yet both processes are important to understanding the role of technology in generating a mobilisation of resistance against disinformation.

Legitimation is an interactive, political process that takes place between actors in which one actor seeks to justify their identity, interests, practices, or institutional designs in exercising authority over another (Gronau and Schmidtke, 2016: 537–539; Reus-Smit, 2007). However, when applied to whole-of society-resistance to disinformation, legitimation must account for the emotional and spiritual dimensions that exist within the relationship between a populace and its governing elites. This is because disinformation campaigns target these dimensions by seeking to enflame public suspicion and outrage towards state representatives. When applied to resistance against disinformation, legitimation is best understood as an active process involving the 'crystallisation of several beliefs . . . which are untouchable, and which affect the total conduct of actors in a significant but diffuse manner' (Bourricaud, 1987: 64). Belief targets the subjective state of the believer: 'belief is a persuasion which involves not only intellectual elements but also moral ones' (Bourricaud, 1987: 64–65). In the context of democracy, legitimation must involve convincing the public that democratic systems care about their needs and are capable of meaningfully addressing them.

Denmark's response to the global outbreak of COVID-19 presents a case of legitimation facilitated by sociotechnical systems. A survey of 14,000 respondents across 14 advanced economies in Europe indicates Denmark received the highest government approval rating among citizens in terms of their country's pandemic response and its impact on national unity (Wood, 2020). Two studies highlighted that Denmark's swift, early restrictions as well as the administration's decision to take full responsibility for all actions contributed to greater public trust in the government (Nord and Gardell, 2023: 62; Nielsen and Lindvall, 2021). Danish citizens appeared more persuaded by their state representatives' ability to handle COVID-19 compared to citizens of other countries. Technologies played a role in facilitating this legitimation, from daily televised press conferences as well as the country's 'Recovery and Resilience Plan' which improved data management in the Danish health service and digitalised patient treatments through tele-medicine and electronic patient records (European Commission, 2021).

If governing elites can inspire sufficient belief across a society, they can reinforce a mobilisation of resistance against disinformation in which they carry greater legitimacy in their ability to govern and exercise power, thereby diminishing the possibility of public mistrust or outrage. The process of legitimation can therefore be considered part of whole-of-society resistance to disinformation. As for its link to technology, legitimation is a potential biproduct of successful co-production in the sense that it results in public trust in state representatives. Yet unlike enframing and co-production, legitimation is less concerned with the agency of technologies and more so with the agency of society in choosing whether to trust political representatives. Legitimation also differs from the other processes in the way it highlights how resistance to disinformation narratives might occur at an *affective* level by inspiring citizens' belief in elites' ability to govern through intellectual and moral persuasion. Legitimation thus illustrates another process through which a mobilisation of resistance may be consolidated, thereby reducing a society's susceptibility to anti-elite narratives propagated by transnational disinformation campaigns.

Humour

The capacity of humour to act as a mechanism of resistance in challenging power has been widely observed within International Studies (Baspehlivan, 2024; Bhungalia, 2020; Browning and Brassett, 2023; Malmvig, 2023; Wedeen, 1999). Akin to legitimation, humour addresses another affective dimension through which resistance to the power of transnational disinformation can be expressed. This is because humour is a metacommunicative process[5] through which power relations can be altered at the affective level. This relates to the state as power is partly predicated upon the affective dynamics between the powerholder (A) and the less powerful (B) in the social construction of identity and the extent to which A and B invest in these identities underpinning the power relationship (Solomon, 2014: 2). For instance, A's success in exercising power upon B through appeal results from 'representation acts that symbolise shared worlds' through language and identity (Hayden, 2012 [2011]: 45; Solomon, 2014: 2). Humour can therefore either alter or reinforce the extent to which these symbolised worlds are shared between A and B. Simply put, humour can shape the subject's perception of their own identity in relation to a powerholder and to what extent the subject buys into that identity. This highlights humour's double-edged 'productive power' in affirming solidarity among certain communities, while 'othering' groups beyond those bounds (Browning and Brassett, 2023: 174; Malmvig, 2023: 514).

Technologies structure how the productive power of humour is exercised, especially online. Sociotechnical systems pluralise modes of civic engagement and political expression, as well as generate modalities of expression and connection within the cyber sphere (Papacharissi, 2014: 26). STS has long held the view that technology is 'a complex enterprise that takes place in specific contexts shaped by and, in turn shaping, human values' (Bowden, 2002 [1995]; Cutcliffe, 1989: 70). Humour through online memes and the resonance of that humour enabled by the algorithms of sociotechnical systems form part of this enterprise and therefore play a part in shaping such values. This is achieved through the inclusion of discourses and actors as 'humorous' as well as the construction of online communities in which these identities between actors are reinforced, sometimes in nation-specific projects.[6] For example, the productive power of humour can be channelled through sociotechnical systems to reinforce a state's mobilisation of resistance against disinformation. Take for instance the Ukrainian Ministry of Defence's X/Twitter page (@DefenceU), which frequently posts humorous memes aimed at debunking Russian disinformation stressing 'superior' Russian military capabilities as seen in Figure 1 (2022).

The Ukrainian state uses humour to *organise out* narratives of Russian military strength and competence while *organising in* solidarity with Ukrainian citizens as well as the international community through debunking (Tokariuk, 2023). If shared widely, humorous memes can *organise out* misleading discourses introduced by the disinformation through ridicule on the one hand, while *organising in* certain identities across a community on the other hand. Humour facilitated through sociotechnical systems like memes therefore presents another process through which a mobilisation of resistance against transnational disinformation can be forged between states and the societies they govern.

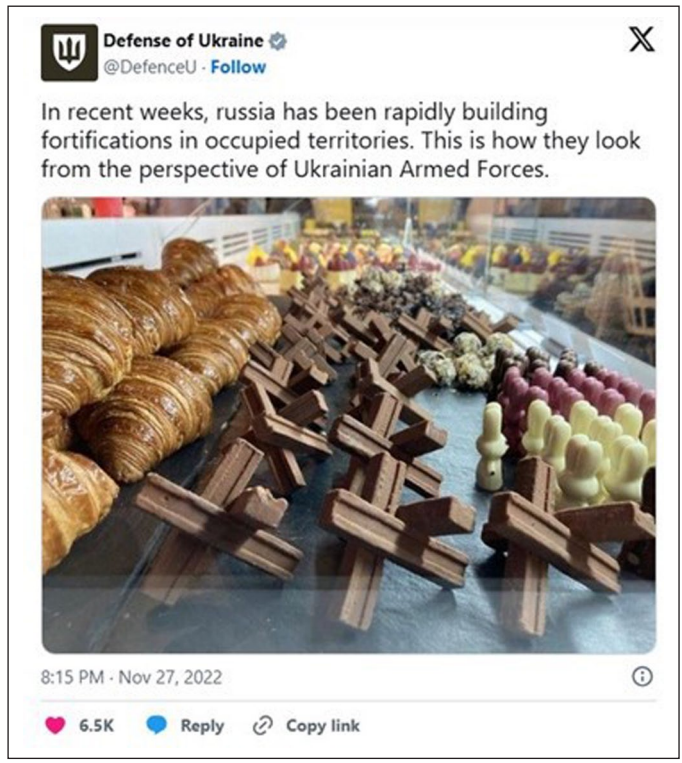


Figure 1. An image posted by the Ukrainian Ministry of Defence on X/Twitter of Kyiv's Honey Café bakery selling chocolate versions of anti-tank hedgehogs (Tokariuk, 2023: 20).
Source: Ukrainian Ministry of Defence (2022).

Taiwan's OSG and ACG as paradigmatic cases of sociotechnical resistance

This article examines two types of sociotechnical systems: open-source governance (OSG) and algorithmic co-governance (ACG). 'Open source' refers to practices in the production and development of sociotechnical systems that promote access to the end product's source materials to enable peer review for innovation and creation of more effective products (Matei and Irimia, 2014: 812). Based on an open-source approach, OSG is defined as a type of governance that

> promotes the usage of open-source production and development models as modus operandi for engaging citizens constructively across the boundaries of public agencies and levels of government, in order to enhance, via IT platforms acting as a go-between, the design and implementation of public policy, goods, and services. (Matei and Irimia, 2014: 813–814)

This form of governance manifests in the social sphere in '[acts] of collaboration in an open-source way' (Matei and Irimia, 2014: 812). These acts are broadly characterised by two stages of collaboration: (1) regular users identifying and reporting 'bugs' (errors or

flaws) in products and (2) actors with IT skills co-producing software by submitting 'patches' (pieces of code designed to fix problems or enhance functionality) (Matei and Irimia, 2014: 813). In line with its commitment to transparency and accessibility, open-source collaboration can also involve rendering complex information more intelligible. In an OSG context this is often aimed at maximising public engagement with the political process.

Algorithmic co-governance (ACG) is characterised by collaborative coding. Algorithms are encoded procedures which seek to solve problems 'by transforming input data into a desired output' (Yeung, 2018: 506). Co-governance is a process whereby social actors join hand with a common purpose in mind and stake their identity and autonomy in the process (Kooiman and Jentoft, 2009: 821). ACG manifests as horizontal, interconnected networks where there are high levels of power-sharing, inter-dependence and negotiation (Gritsenko and Wood, 2022: 55–57). Algorithmic governance involves systems of algorithm-based decisions which utilise large datasets maintained by tech-savvy actors to the inform bureaucratic decision-making systems (Danaher et al., 2017: 2). OSG and ACG are sociotechnical systems which are structured to promote transparency, collaboration, accessibility and participation.

Taiwan proves an instructive case in whole-of-society resistance to transnational disinformation campaigns through OSG and ACG technologies. Many studies have documented how Chinese state-sponsored interference activities overseas seek to influence the domestic environments of other countries in ways that are favourable to the advancement of the Chinese Communist Party's (CCP) foreign policy goals (Brady, 2018; Chan and Alden, 2023; Groot, 2018; Hackenesch and Bader, 2020; Hughes, 2015; Kaul and Thornton, 2025). Taiwan has long been at the forefront of these activities (Barss, 2022; Brady, 2015; Cheravitch, 2025; Cole, 2021; Rawnsley, 2016; Templeman, 2020; Wang et al., 2020; Zhang, 2022). Taiwan has experienced decades of intense and sustained pro-unification propaganda campaigns from China in the form of 'united front work' (統戰工作 *tongzhan gongzuo*) which target pro-Chinese factions within Taiwanese society and politics, seek to cast the CCP in a positive light, advance CCP ideology across Taiwanese society, convince Taiwanese people of the 'inevitability' of unification with China, as well as encourage Taiwanese people to identify as 'Chinese'. With the advent of social media coinciding with Taiwan's democratisation in the 1990s and early 2000s, the country has become a testing ground for China's transnational disinformation campaigns and 'cognitive warfare' (認知戰 *renzhi zhan*) (Cheng et al., 2023; Haciyakupoglu and Raska, 2021; Huang, 2023; Hung and Hung, 2020; Kao, 2021). In recent years, CCP disinformation activities have been aimed at intimidating Taiwanese people and stoking distrust towards the Democratic Progressive Party (DPP) government which is perceived by the Chinese state to be pro Taiwanese independence (Cheng et al., 2023). For example, when COVID-19 struck Taiwan in early 2020, viral posts emerged falsely claiming the United States refused to sell Taiwan 'a single vial of vaccine', that tens of thousands of Taiwanese people were travelling to China to receive the vaccine due to domestic shortages, and that Taipei had plans to offer vaccines to diplomatic allies despite not having enough to vaccinate its own population (Hille, 2021). Similarly, following a national egg shortage, public dissatisfaction in Taiwan fuelled by disinformation narratives of egg hoarding by retired teachers and sales of artificial eggs arguably led to the resignation of the Minister of Agriculture (Taiwan AI Labs, 2024: 12).

In the face of China's persistent disinformation campaigns, the Taiwanese state, media and civil society organisations have all contributed to a strong mobilisation of resistance by creating tools to identify CCP disinformation and united front work, educating the public about these activities and maintaining standards in the information ecosystem. I argue the Taiwanese civic tech community g0v[7] reflects the sociotechnical expressions of this mobilisation of resistance. G0v has developed open-source technologies and co-governance platforms to improve democratic processes as well as counter disinformation. The group was formed in 2012 when a group of Taiwanese self-described civic hackers built an online system for netizens to audit the central government budget more effectively. During the 2014 Sunflower Movement, g0v gained popularity due to its use of digital technologies to resist perceived anti-democratic measures under the Ma Ying-jeou Kuomintang administration (2008–2016) as well as China's growing influence in Taiwanese domestic affairs. Closely linked to open source and OSG, the g0v community's ethos and practice of 'open culture' (開放文化 *kaifang wenhua*; Open Culture Foundation 開放文化基金會 Personnel, 22 August 2023) centres on the belief that governance and civic activity should be transparent, intelligible, accessible, collaborative, inclusive and aimed at delivering a 'public good' (g0v, 2019; Billion Lee, Co-facts founder and gov member, Interview, 28 June 2023

Under the Tsai Ing-wen administration (2016–2024), the government incorporated OSG and ACG into its governance by establishing the Ministry of Digital Affairs (MoDA) and open culture committees which support government ministries to digitalise their operations as well as explore applications of open culture principles and OSG/ACG sociotechnical systems to their respective policy fields. These activities seek to enhance the operations of Taiwanese government ministries on the one hand while arguably bolstering the resilience of Taiwanese democracy to withstand CCP disinformation and united front work activities on the other hand. Taiwan's OSG and ACG technologies therefore present paradigmatic cases of whole-of-society resistance to disinformation through sociotechnical systems (Cheng et al., 2023; Flyvbjerg, 2006: 230). The next section features empirical examples which highlight the four processes through which Taiwan has carried out resistance to CCP disinformation: (1) enframing, (2) co-production, (3) legitimation and (4) humour.

Resistance through enframing: co-facts

The g0v fact-checking search engine and chatbot CoFacts (真的假的 *zhende jiade*) represents a case of resistance to disinformation through enframing. According to CoFacts's social impact report, its search engine receives 45,000 searches per week, a total of 10 million page views per year, while the chatbot responds to 200,000 reports of potential disinformation per year (CoFacts Special Impact Report). If a user encounters what they suspect might be a link to disinformation, they can input the link into the CoFacts search engine or forward it to the CoFacts chatbot through the messaging application LINE. The search engine and chatbot have been programmed with artificial intelligence (AI) that follows a strict fact-checking procedure. The AI is structured to identify and categorise information within linked news reports according to 'fact' and 'point of view',

cross-reference claims across a range of news sources, and offer an overall evaluation of the narrative's credibility. CoFacts users can also report potential cases of dis/misinformation which are then examined by a physical fact-checker who implements the same fact-checking procedure as the AI.

Above is a response from the CoFacts chatbot to the YouTube video 'Tim Clissold: No language like Chinese is one reason Europe can't unify'. In the video, Tim Clissold claims the 'core' of the Chinese civilisation dating 2,000 years ago has endured while Europe's core collapsed during the fall of the Roman empire, positing that 'Europe's basic problem at the moment is unification'. The response from the CoFacts Chatbot identifies four points that 'warrant special attention', such as the video communicating only Clissold's point of view that the lack of a language such as Chinese was one of the reasons why Europe could not be united. The chatbot response explains 'no concrete evidence or research has been provided to support this viewpoint' and concludes: '*The source of this message is unclear and cites personal opinions without concrete evidence to support them. Listeners should remain sceptical and conduct their own in-depth research and verification to ascertain the authenticity and credibility of the message*' (see Figure 2).

Above is a CoFacts fact-checker's response to a report of potential dis/misinformation about COVID-19 drawn from a popular online post in 2020. The fact-checker identifies claims made in the post such as 'vaccine development is much slower than virus mutation' and 'the virus has mutated three new attack pathways' as dis/misinformation. The fact-checker then provides sources from the World Health Organization and the Harvard Centre for Communicable Disease Dynamics to confirm their corrections to the dis/misinformation. Users can then vote on whether the fact-checker's sources, analysis and overall evaluation were 'helpful' or 'unhelpful' (see Figure 3).

Both examples highlight how technology enframes resistance to disinformation by converting information encountered by users into a wider system of fact-checking. The evaluations provided by the AI chatbot and physical fact-checkers are designed to be brief, straightforward and easy to understand. This conversion of information and discourses into an evaluation informed by fact-checking facilitates resistance towards 'suspicious' information and rumours when it is encountered by users of the technology. The evaluation also drives out other possible interpretations of the information to the user, naturalising the process of fact-checking, which inherently involves *organising out* dubious information and discourses using a set of pre-determined categories, such as fact versus point of view. CoFacts, alongside other fact-checking services promoted by the DPP government such as Taiwan Factcheck Center, Rumour & Truth and MyGoPen (Ministry of Education, 2023), therefore contribute to building a mobilisation of resistance against Chinese disinformation across Taiwanese society.

Resistance through co-production: vTaiwan

The g0v sociotechnical process vTaiwan demonstrates how technology has the potential to produce a democratic social order which minimises the mistrust towards state officials and processes that disinformation campaigns seek to advance. vTaiwan utilises the software Pol.is which engages in 'consensus-mining': generating a rough consensus on a topic among a group of participants. The vTaiwan process recruits representatives of different social groups to work together to resolve policy issues through consensus-mining.

Figure 2. The CoFacts chatbot responds via the messaging application LINE to a YouTube video link titled 'Tim Clissold: No language like Chinese is one reason Europe can't unify'.
Source: CoFacts Chatbot via LINE, received by the author on 8 November 2023.
Translation: '*This piece of information contains several points which merit special attention and scrutiny. 1. The source: The information fails to provide an exact source; it only refers to news circulating online. For this reason, we have no way of confirming the reliability and veracity of the information. 2. The perspective of Tim Clissold: this piece of information only refers to Tim Clissold's perspective which claims that one of the reasons why Europe could not unify is due to a lack of unifying language like Mandarin. However, this represents only the perspective of Tim Clissold, it doesn't provide any specific evidence or research to support his point of view. For this reason, we must be cautious when faced with this type of advocation. 3. The response of Tim Clissold: Tim Clissold states that "No language like Chinese is one reason Europe can't unify," but none of Clissold's background qualifications or sources are provided. Due to this, we have no way of confirming the reliability or veracity of this response. In summary, the sources for this piece of information are unclear, it uses only personal opinions and lacks specific evidence to support these opinions. Listeners should maintain a sceptical position and carry out their own in-depth research and verification to ascertain the veracity and reliability of this piece of information*'.

vTaiwan involves online and face-to-face dialogues about policy issues between stakeholders, government representatives and members of the public. These dialogues are organised according to the 4-step 'focused conversation method': (1) collecting open and

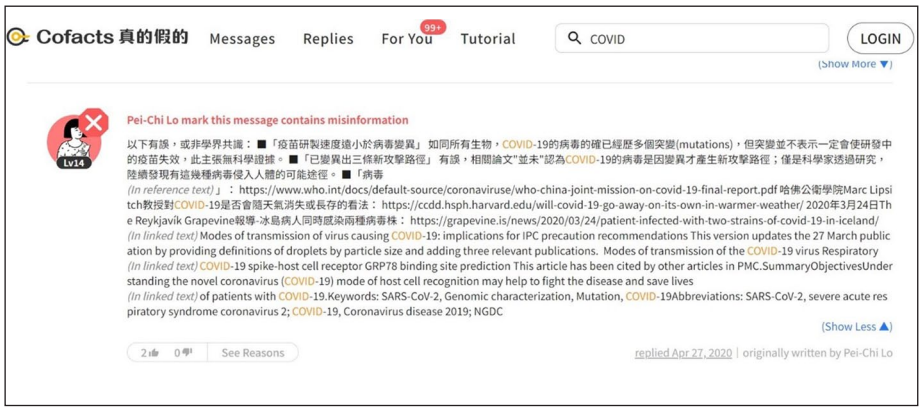


Figure 3. A CoFacts fact-checker responds to a report of dis/misinformation about COVID-19.
Source: Lo (2020).
Translation: '*The following claims contain falsehoods and or a lack of scientific consensus: "The speed of vaccine development is far slower than the virus mutation." Just like all living things, the COVID-19 virus certainly has undergone several mutations, but these mutations do not mean that the vaccines being developed will be ineffective against the virus. [. . . but this doesn't make the vaccines that are being developed ineffective]. This point of view lacks scientific evidence. The claim that "mutations have produced three new attack pathways" also contains falsehoods. Related texts "have not yet" found the COVID-19 virus produces new attack pathways due to mutations. Yet, research carried out by scientists has gradually discovered additional pathways of viruses to infect people*'.

objective data as well as firsthand experiences, (2) identifying feelings about those facts, (3) generating ideas that resonate most with people's concerns and (4) making decisions that address those concerns (Gov Lab, 2019; Tang, 2017). During the dialogue and based on the Pol.is results, government representatives can respond to common concerns among participants towards a policy or its implementation. In some cases, officials have drafted regulations based on the results of the consensus-mining and dialogue. Draft regulations were resubmitted to vTaiwan for further scrutiny and input from the public and key stakeholders, sometimes undergoing several rounds of revision (Atlee, 2018).

Pol.is is a software deployed within the vTaiwan process which collects the opinions of participants on a policy issue and maps areas of rough consensus through advanced statistics and machine learning (Pol.is, 2024). Through Pol.is, netizens submit short statements in a dialogue box expressing their views about a policy issue. These statements are then voted on by other participants who choose to 'agree', 'disagree' or 'pass'. After collecting these votes, the Pol.is algorithm generates a map depicting 'opinion clusters' which are organised according to the statements which received the highest levels of agreement among participants. These results are then discussed in face-to-face dialogues. These dialogues, along with the rough consensus map drawn by Pol.is, then inform the drafting of legislation by government ministers. As of October 2023, vTaiwan has been used in 23 policy consultations, 20 of which resulted in either a new law or an amendment (Former Member of the Participation Officer Network, Interview, 1 March 2024). According to a 2019 report, over 200,000 people have participated the vTaiwan process to identify and address public concerns towards complex policy issues (Gov Lab).

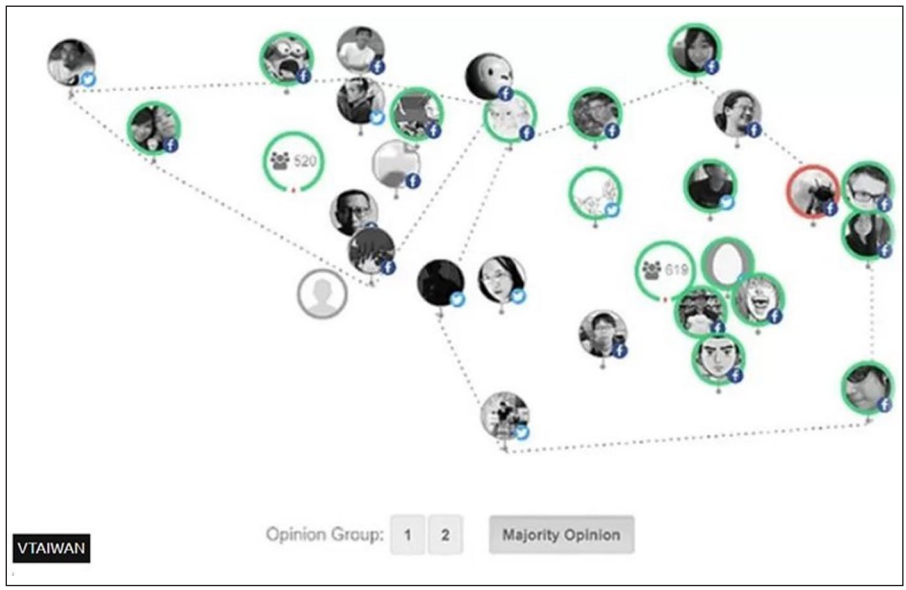


Figure 4. A map of a rough consensus generated by the software Pol.is which grouped together participants based on their response to statements about the implementation of Uber in Taiwan. *Source*: Miller (2019).

In 2015, vTaiwan and Pol.is were used to address the issue of regulating Uber in Taiwan. Pol.is collected the opinions of 1,875 online participants, including members of the public, industry leaders, academics, as well as representatives from Association of Taxi Drivers in Taipei, Taiwan Taxi, Uber Inc., and the Ministries of Transport, Economic Affairs, and Finance. The results of the Pol.is survey identified a rough consensus that reflected two recurring concerns among participants in regulating Uber: (1) outlawing unlicensed passenger vehicles and, (2) ensuring the domestic taxi industry was able to compete with Uber by raising their management quality control systems to the same standard (see Figure 4). Based on these results, the government implemented regulations which allowed for non-yellow taxis, required Uber driver registration, increased information requirements for app-based dispatch systems, and made it compulsory to report per-ride taxation to the Ministry of Finance (Tang, 2016, 2017). In addition to Uber, the vTaiwan system was applied to 22 other policy issues shown in Figure 5, including drafting and updating regulations on revenge porn (Former Member of the Participation Officer Network, Interview, 1 March 2024).

vTaiwan therefore represents a form of co-production on two levels. First, its emphasis on transparency, participation, consensus-mining and its applications of these to legislation indicate it is a sociotechnical process shaped by a democratic social order. This is because vTaiwan was created by g0v to make the legislation process more transparent, participatory and effective in addressing peoples' concerns, or as former Digital Minister

Policy Issues	Date	Legislative Change
Introducing uber to taiwan	201507-201610	yes
Cyberbullying	201506-201508	no
Telework	201503-201605	yes
Telemidicine	201503-201506	yes
Online shopping standard contract	201503-201610	yes
Tax on online transations	201502-201610	yes
Crowdfunding	201502-201503	unclear
Regulations on "close corporations" (common for startups)	201502-201505	yes
Data Levy fee	201503-201605	unclear
Regulatory sandbox	201702-201712	yes
Airbnb/ short term rental	201509-201711	yes
Regulations on drone flying	201706-201804	yes
Regulations on e-clinic	201708-201805	yes
Regulations on remote education	201504-201807	yes
Regulations on information security	201506-201806	yes
Developments on sharing economy	201706-201805	yes
Translating company names into English	201608-201808	yes
Regulations on social enterprise	201612-201808	yes
Regulations on board of directors election	201702-201808	yes
Regulations on uncrewed vehicle	201708-201812	yes
Regulations on electric personal assistive mobility device	201907-202205	yes
Nonconsensual pornography	201707-202302	yes
Open parliament	202008-202211	yes

Figure 5. A table depicting the 23 policy consultations where vTaiwan was applied and indicating whether the process resulted in a change to the relevant legislation.
Source: Former Member of the Participation Officer Network, Interview, 1 March 2024.

Audrey Tang summarised: 'take care of peoples' feelings' (Tang, 2017). Both vTaiwan and the Pol.is software facilitated participation in law-making through technology, reflecting gov's open culture values. This represents the social production *of* technology within co-production. Second, through OSG and ACG practices, vTaiwan reinforces a democratic social order by building users' trust in the legislative process. vTaiwan participants and the wider public might feel more invested in policymaking if it addresses their concerns. This represents the social production *by* technology. This *organises in* participants' trust in policymaking, likely making them more sceptical towards common disinformation narratives that seek to portray the Taiwanese government as incompetent or neglectful of citizens' needs, or that would inspire mistrust in democracy in general. This contributes to a mobilisation of resistance which *organises out* mistrust towards governing elites over the long-term and *organises in* trust towards policymaking and the government officials overseeing it. As disinformation seeks to subvert states' structural power, vTaiwan represents a case of sociotechnical resistance to disinformation through democratic co-production which bolsters structural power through democratic co-production.

Resistance through legitimation: LINE FactChecker

The fact-checking platform sponsored by the Taiwanese government on the popular messaging application LINE presents a case of resistance to disinformation through legitimation. LINE remains the most dominant instant messaging application in Taiwan. There are around 21.68 million LINE users (Kemp, 2023), and it accounts for approximately 77.56 percent of the country's market share in the messaging application sector as of May 2023 (Statista). In 2019, it was estimated over 9 billion messages were sent via the messaging application per day (LINE, 2022). Recognising that existing Taiwanese fact-checking organisations could not keep pace with the volume of disinformation narratives spreading on messaging platforms, LINE partnered with the government's Executive Yuan News Bureau under the Digital Accountability Project to create a centralised, official platform for fact-checking and verified news called 'LINE FactChecker' (Former Member of the Participation Officer Network, Interview, 1 March 2024). This government platform incorporated data and reports of disinformation across a range of government and civil society fact-checking organisations including the 'Executive Yuan Clarification Zone', the Taiwan Factcheck Center, Rumour & Truth, MyGoPen and CoFacts (Lange and Lee, 2020). By adding LINE Message Verification as a contact, LINE users could access government approved fact-checking services and track trending disinformation narratives. Like the CoFacts chatbot and search engine, users can forward text messages and links they suspect to be disinformation to the official account for verification. However, unlike CoFacts, these verification services are directly linked to the state. The LINE FactChecker is specifically aimed at bolstering citizens' belief in the government's competency to address dis/misinformation and scams, while non-governmental fact-checking services centre on maintaining standards in the broader information ecosystem. If the messages or links have been verified by one of the above fact-checking services, the account replies directly with the results, while unverified messages and links are reported to the verification unit. Once the unit has evaluated the message or link, users receive a notification from the platform. As of April 2022, the platform has seen a total of 1,330,000 visits (LINE, 2022).

The platform also links to the LINE FactChecker website (https://fact-checker.line.me/) so users can check the full list of verified news, including trending news under 'TOP 10 Topics', government-related news under 'Public Affairs' and 'Topics by Category'.

On the 'Public Affairs' LINE webpage depicted in Figure 6, Taiwanese government ministries post reports which address trending dis/misinformation relating to their policy jurisdictions.

The LINE Message Verification platform represents a sociotechnical system specifically aimed at persuading citizens' belief in policymakers' ability to address public concerns and govern effectively. The government's LINE Message Verification, in collaboration with fact-checking NGOs, seeks to provide assurance to LINE users that the government is consistently monitoring forms of dis/misinformation that could potentially harm citizens across various policy areas.

The message verification platform played an important role in government communications with the public during the outbreak of COVID-19, with the average daily number of visitors to the message verification platform increasing by approximately 3.6 times

Figure 6. A screenshot of the LINE FactChecker platform.
Source: LINE FactChecker (2023).
Translation:
'*Public Affairs*
Ministry of Finance Clarification: Universal Cash Online Registration is strictly encrypted and will be deleted one month after the end of the project.
Control Command Center Clarification: There is no way we can force citizens to get vaccinated.
Ministry of Health and Welfare: Scam email to receive $6,000: Executive Yuan urges you not to click on links from unknown sources.
Executive Yuan: Farm Bureau: $700 Billion in Official Development Assistance (ODA) Funds is Untrue, Don't Believe It, Don't Share!'.

during the height of the outbreak in mid-May of 2021 (LINE, 2022). The platform therefore arguably supported Taiwanese LINE users to resist the influx of CCP disinformation concerning the virus and the government's COVID policies. This highlights the process of legitimation through OSG practices and technologies to *organise in* trust towards officials and state institutions across society.

Resistance through humour: disinformation-debunking memes

Taiwan's OSG approaches also highlight how governing elites deploy humour to illicit a population's affective investment into their governance. The Taiwanese government approach of 'humour over rumour' – a phrase popularised by former Digital Minister without Portfolio Audrey Tang – presents another dimension of resistance to disinformation. Based on OSG approaches, government participation officers (開放政府聯絡人 *kaifang zhengfu lianluo ren*) work within ministries to 'meme-ify' state communications aimed at debunking disinformation within a 20-character title and 200-character mess (Kao, 2021). These memes render the debunking disinformation discourses more intelligible and resonant through humour. This reflects the humour over rumour approach, the idea that humorous messages debunking disinformation can resonate across a high number of netizens, thereby achieving the same impact or virality as the disinformation itself. Humour over rumour represents a form of 'gamification' – the integration of game

Figure 7. A meme created by the Taiwan Ministry of Health and Welfare about social distancing.
Source: Taiwan Ministry of Health and Welfare (2021).
Translation: '*Pandemic or not, don't spit! Remember to maintain social distancing, wash your hands, and wear your facemask properly. The three-dot ellipses demonstrate social distancing. Ministry of Health and Welfare Chief Shina Ibu promotion 2021 January 27th*'.

mechanics into a non-game environment to give it a game-like feel, motivating users to accomplish certain tasks – an approach originating from g0v's open culture aimed at incentivising public participation in a project (Lien et al., 2021).

In response to an influx of disinformation since Taiwan's first reported case of COVID-19 in January 2020, participation officers used humour in public health communications to dispel common disinformation narratives about the virus, make the government's COVID policies intelligible and memorable to the general public and portray the government in a proactive light (Former Member of the Participation Officer Network, Interview, 1 March 2024). This was part of a broader government effort to maintain public trust in the official handling of the pandemic through consistent and transparent communication, for example, by providing daily updated statistics on the number of deaths and cases of COVID-19 according to locale. Humour was used to make government policies about the virus easy to understand and remember. One example of this is the 'three Shina Ibu' meme used to illustrate the Ministry of Health and Welfare's (MoHW) guidance on social distancing:

The Shina Ibu, named 'Zongchai' which roughly translates to 'Chief Shina Ibu', remained a consistent theme in MoHW public communications about COVID-19 (see Figure 7). Though it is difficult to measure the extent to which the humorous official messaging was well-received by Taiwanese citizens, especially 'deep blue' communities

Figure 8. A meme created by the Taiwan Ministry of Foreign Affairs encouraging application to Mandarin study programmes in Taiwan.
Source: Hale (2022).

sceptical of the DPP, studies indicate the government's communications strategy on social media received greater engagement through likes and shares (Lien and Wu, 2021), while public approval of the Tsai administration's countermeasures against COVID-19 reached 84 percent in the early stages of the pandemic (TVBS Poll Center, 2021).

Similarly, to resist a CCP-led campaign which pressured overseas organisations to change the designation of Taiwan on their websites and drop-down menus to the misleading 'Taiwan, China' or inaccurate 'Taiwan, Province of China', the Taiwanese Ministry of Foreign Affairs (MoFA) created this meme in a post about scholarships to study in Taiwan:

The image utilises the popular meme of rap artist Drake rejecting an idea in one frame then endorsing a contrasting idea in the next frame (see Figure 8). The meme parodies the CCP inaccurately designating Taiwan as a territory of China by referring to China as 'West Taiwan'. The meme also refers to China as *kou guo* or 'mouth country' to poke fun at Chinese censors replacing the term 'kill' in American TV series with 'mouth' (*kou*) for Chinese audiences in 2022. Humour over rumour illustrates the OSG approach to debunking and resisting disinformation narratives. When successfully applied, humour can *organise out* misleading disinformation narratives through ridicule as well as mistrust for governing elites on an affective level, and *organise in* solidarity between the public and the state in resisting interference.

Conclusion

As several democratic elections unfolded over the previous year, the question of how states and their societies can collaborate to resist transnational disinformation campaigns

remains a recurring issue in global politics. This article begins with the simple observation that since civil societies and social technologies constitute the terrains upon which transnational disinformation campaigns subvert state power, they must also be the sources through which whole-of-society resistance to this subversion can be enacted. Developing this observation further, this article leverages insights from Social Theory and Science and Technology Studies (STS) to posit a social-processual framework through which one can examine the agency of society and sociotechnical systems in contributing to whole-of-society resistance against transnational disinformation campaigns. The mobilisation of bias shows how agenda-setting by states and civil society actors can be a long-term strategy to resist disinformation and build democratic resilience, something I have termed the 'mobilisation of resistance'. Expanding this framework further, this article has shown that a mobilisation of resistance can be structured through sociotechnical systems and the processes of enframing, co-production, legitimation and humour.

The case of Taiwanese whole-of-society resistance through open-source governance (OSG) and algorithmic co-governance (ACG) sociotechnical systems illustrates how civil society actors and technologies have agency in facilitating a pro-democratic mobilisation of resistance against disinformation campaigns. The empirical analysis explored how states can work with civil society actors to structure sociotechnical systems to resist transnational disinformation as well as encourage public participation and trust in democratic governance. OSG and ACG sociotechnical systems can be harnessed to expedite the identification of disinformation through fact-checking as well as foster transparency, participation and collaboration across state-society relations through democratic agenda-setting.

Overall, this article offers four potential contributions to the field of IR. First, the theoretical framework of a mobilisation of resistance lends explanatory power to cases of whole-of-society resistance against transnational disinformation occurring in other contexts beyond Taiwan such as Ukrainian and Estonian resistance to Russian disinformation. Second, the social-processual approach advanced in the analysis presents a theoretical perspective which allows scholars of disinformation to account for the roles of non-state actors in resisting disinformation as well as the broader cultural, social and historical forces which explain why disinformation narratives might be impactful in certain contexts but met with resistance in others. Third, the article puts the IR disinformation literature in conversation with STS and Social Theory to enrich the field's ability to explain the positive, active roles societies and social technologies can play in mitigating the harms of transnational disinformation campaigns to states and the societies they govern as well as (re)producing social orders. STS highlights technologies' capacity to not only disrupt but also cultivate social orders while Social Theory provides insights into the variety of ways in which resistance is expressed as well as how social trust is reinforced, an antidote to the outrage and suspicion that disinformation campaigns seek to enflame. These insights speak to ontological security concerns over the maintenance of state identity by demonstrating how technologies can have a positive bearing on the power and resilience of states to withstand transnational subversion. The mobilisation of resistance framework therefore empowers the IR disinformation literature to go beyond simply indexing the harms of transnational disinformation to states and explore how

states might meaningfully *resist* these activities by collaborating with civil society actors and utilising technologies. Fourth, this article builds on relational approaches to resistance within IR (Bourbeau and Ryan, 2018) by exploring how the agencies of societies and sociotechnical systems interact to articulate whole-of-society resistance. Broadly speaking, the four processes of enframing, co-production, legitimation and humour may contribute to literatures advocating for relational and processual approaches to resistance as well as address calls to further examine the relationships between the state, society, technology and power.

While this article centred its analysis on OSG and ACG technologies, sociotechnical systems present just one way in which a pro-democratic mobilisation of resistance against transnational disinformation can be achieved. In refining this framework further, researchers could unearth other modalities of resistance against disinformation through education policies or cyber security systems. In addition, scholars could consider cases of resistance to disinformation in contexts where there are many polarising issues or in societies with limited or no access to OSG and ACG sociotechnical systems. On a methodological level, qualitative and quantitative research methods could potentially be applied to measure the impact of the mobilisation of resistance.

Acknowledgements

I would like to specifically thank the following individuals for their insights and encouragement which contributed to the publication of this paper: Luca Tardelli, Chris Alden, Rohan Mukherjee, Tomila Lankina, Stefano Guzzini, Katharine M Millar, Alex Stoffel, Yi-Ting Lien, Felix Brender-Wang, Charlie Carter, and Chris Deacon. I am especially grateful to my colleagues Andrea Hanlun Li and Sophie Kaldor for their close reading of the manuscript in preparation for its first submission. Previous versions of this paper were presented at the BISA International Studies and Emerging Technologies (ISET) group in May 2022, the LSE's IR504, IR502, and Colloquium workshops, as well as the Hoover Institute's Project on Taiwan in the Indo-Pacific Region (PTIP) workshop in May 2023. My thanks to all the discussants and participants who offered thoughtful feedback which contributed to the development of this paper. Finally, I wish to express my gratitude to the editors and two anonymous reviewers for their feedback which helped sharpen the theoretical and empirical contributions of this article.

Declaration of conflicting interests

The author(s) declared the following potential conflicts of interest with respect to the research, authorship and/or publication of this article: Some of the empirical examples and interviews presented in the paper were collected during fieldwork in 2023 which was funded by the Taiwan Fellowship, a scholarship established by the Taiwan Ministry of Foreign Affairs.

Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.

ORCID iD

Mariah Thornton https://orcid.org/0000-0002-1505-0911

Notes

1. The analysis presented also seeks to shed light on the following sub-questions: What is the relationship between the state, society, resistance and technology? and Can democratic resistance be materially enacted through sociotechnical systems?
2. Abbott stresses the 'historicality' of the individual by treating them as a 'reservoir of historical connection from past to present' (2016: 5).
3. Lukes (1974) describes the third face of power as the ability to influence, shape and determine a subject's wants and perceptions of their own wants.
4. Strands within STS emphasise sociology while others favour traditional philosophy (Restivo, 2007 (1995): 109). For example, though prominent STS scholar Latour criticised Heidegger as a pessimistic technological determinist (Latour, 1999: 176; Ma and Van Brakel, 2014), Heidegger's concept of enframing (*ge-stell*) has nevertheless impacted theoretical developments within STS (see Borgmann, 1984; Ciborra, 2004).
5. See Brock (2010).
6. Sociotechnical imaginaries refers to the collectively imagined forms social order reflected in the design and fulfilment of nation-specific scientific and or technological projects (Jasanoff and Kim, 2009: 120).
7. Pronounced 'gov zero'.

References

Abbott A (2016) *Processual Sociology*. Chicago, IL: University of Chicago Press.

Anzera G and Massa A (2021) Using International Relations theories to understand disinformation: soft power, narrative turns, and new wars. In: López-García G, Farpón CR, Calvo D, et al. (eds) *Politics of Disinformation: The Influence of Fake News on the Public Sphere*. Hoboken, NJ: John Wiley & Sons, pp. 35–47.

Atlee T (2018) vTaiwan- A glimpse of open-source open space government (Parts 1, 2, 3, 4, and 5). In: *Random Communications from an Evolutionary Age Blog*. Available at: http://www.tomatleeblog.com/archives/175327876 (accessed 1 December 2021).

Bachrach P and Baratz MS (1962) Two faces of power. *The American Political Science Review* 56(4): 947–952.

Barnett M and Duvall R (2005) Power in International Politics. *International Organization* 59(1): 39–75.

Barss E (2022) *Chinese Election Interference in Taiwan*. New York: Routledge.

Baspehlivan U (2024) Theorising the memescape: the spatial politics of Internet memes. *Review of International Studies* 50(1): 35–57.

Bhungalia L (2020) Laughing at power: humor, transgression, and the politics of refusal in Palestine. *Environment and Planning C: Politics and Space* 38(3): 387–404.

Blitz M (2014) Understanding Heidegger on Technology. *The New Atlantis* 41: 63–80.

Bolton D (2020) Targeting ontological security: information warfare in the modern age. *Political Psychology* 42(1): 127–142.

Borgmann A (1984) *Technology and the Character of Contemporary Life: A Philosophical Inquiry*. Chicago, IL: University of Chicago Press.

Bourbeau P and Ryan C (2018) Resilience, resistance, infrapolitics and enmeshment. *European Journal of International Relations* 24(1): 221–239.

Bourricaud F (1987) Legitimacy and legitimization. *Current Sociology* 35(2): 57–67.

Bowden G (2002 [1995]) Coming of age in STS: some methodological musings. In: Jasanoff S, Markle GE, Peterson JC, et al. (eds) *Handbook of Science and Technology Studies*. Thousand Oaks, CA: Sage, pp. 64–79.

Brady A-M (2015) Unifying the Ancestral Land: the CCP's 'Taiwan' frames. *The China Quarterly* 223(2015): 787–806.

Brady A-M (2018) China in Xi's 'New Era': New Zealand and the CCP's 'magic weapons'. *Journal of Democracy* 29(2): 68–75.

Brock A (2010) Humour as a metacommunicative process. *Journal of Literary Theory* 3(2): 177–193.

Browning C and Brassett J (2023) Anxiety, humour and (geo)politics: warfare by other memes. *International Relations* 37(1): 172–179.

Budnitsky S (2022) A relational approach to digital sovereignty: e-Estonia between Russia and the West. *International Journal of Communication* 16(2022): 1918–1939.

Callon M (1987 [1986]) Some elements of a sociology of translation: domestication of the Scallops and the Fishermen of St. Brieuc Bay. In: Law J (ed.) *Power, Action and Belief: A New Sociology of Knowledge?* London: Routledge & Kegan Paul, pp. 196–223.

Chan K and Alden C (2023) <Redirecting>the Diaspora: China's united front work and the hyperlink networks of Diasporic Chinese websites in cyberspace. *Political Research Exchange* 5(1): 1–21.

Cheng H-I, Su C and Su C (2023) A conversation with Taiwan's Minister of Digital Affairs Audrey Tang on communication, technology, identity, and democracy. In: Cheng H-I and Yueh H-S (eds) *Resistance in the Era of Nationalisms: Performing Identities in Taiwan and Hong Kong*. Lansing, MI: Michigan State University Press, pp. 219–236.

Cheravitch J (2025) Commissars with keyboards: the lingering relevance of the military-political origins of Chinese and Russian psychological warfare. *Intelligence and National Security* 40(1): 58–86.

Choucri N and Clark D (2019 [2018]) *International Relations in the Cyber Age: The Co-evolution Dilemma*. Cambridge, MA: MIT Press.

Ciborra C (2004) *The Labyrinths of Information: Challenging the Wisdom of Systems*. Oxford: Oxford University Press.

CoFacts Special Impact Report (n.d.) Taipei, Taiwan: CoFacts. Available at: https://en.cofacts.tw/impact (accessed 9 October 2023).

Cole JM (2021) On the role of organized crime and related substate actors in Chinese Political Warfare against Taiwan. *Prospect and Exploration* 展望與探索月刊 19(6): 55–88.

Cutcliffe S (1989) Science, technology, and society studies as an interdisciplinary academic field. *Technology and Society* 11(4): 419–425.

Danaher J, Hogan MJ, Noone C, et al. (2017) Algorithmic governance: developing a research agenda through the power of collective intelligence. *Big Data & Society* 4(2): 1–21.

Dodds T (2021) Structures of resistance: citizen-generated reporting in times of social unrest. In: López-García G, Farpón CR, Calvo D, et al. (eds) *Politics of Disinformation: The Influence of Fake News on the Public Sphere*. Hoboken, NJ: John Wiley & Sons, pp. 119–131.

Dunn Cavelty M (2010) Cyber-threats. In: Dunn Cavelty M and Mauer V (eds) *Routledge Handbook of Security Studies*. London: Routledge, pp. 263–277.

Dunn Cavelty M (2015) Cyber-security and private actors. In: Abrahamsen R and Leander L (eds) *Routledge Handbook of Private Security Studies*. London: Routledge, pp. 88–99.

e-Estonia (2024) e-Governance. Available at: https://e-estonia.com/solutions/e-governance/e-democracy/ (accessed 1 December 2024).

European Commission (2021) Digital Economy and Society Index (DESI), 12 November. Available at: https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2021

Fallis D (2015) What is disinformation? *Library Trends* 63(3): 401–426.

Farrell H and Newman AL (2021) The Janus face of the liberal international information order: when global institutions are self-undermining. *International Organization* 75(2): 333–358.
Flyvbjerg B (2006) Five misunderstandings about case-study research. *Qualitative Inquiry* 12(2): 219–245.
Frickel S (2014) Not here and everywhere: the non-production of scientific knowledge. In: Kleinman DL and Moore K (eds) *Routledge Handbook of Science, Technology, and Society*. Abingdon: Routledge, pp. 263–276.
Garusi D and Leonhardt B (2024) Towards a processual understanding of trust: a study of trust-building strategies of constructive journalists. *Journalism* 0(0): 1–19.
Gaventa J (1980) *Power and Powerlessness: Quiescence and Rebellion in an Appalachian Valley*. Urbana, IL; Chicago, IL: University of Illinois Press.
g0v (2019) g0v Manifesto 零時政府宣言. *g0v*, 20 October. Available at: https://g0v.tw/intl/en/manifesto/en/
Gov Lab (2019) vTaiwan, *CrowdLaw for Congress*. Available at: https://congress.crowd.law/files/vtaiwan-case-study.pdf
Green J (2015) *Cyber Warfare: A Multidisciplinary Analysis*. Abingdon: Routledge.
Gritsenko D and Wood M (2022) Algorithmic governance: a modes of governance approach. *Regulation and Governance* 16(1): 45–62.
Gronau J and Schmidtke H (2016) The quest for legitimacy in world politics – International institutions' legitimation strategies. *Review of International Studies* 42(3): 535–557.
Groot G (2018) The rise and rise of the united front work department under Xi. *Jamestown Foundation China Brief* 18(7). Available at: https://jamestown.org/program/the-rise-and-rise-of-the-united-front-work-department-under-xi/
Guzzini S (1993) Structural power: the limits of neorealist power analysis. *International Organization* 47(3): 443–478.
Haciyakupoglu G and Raska M (2021) China's political warfare in Taiwan: strategies, methods and global implications. In: Weissmann M, Nilsson N, Palmertz B, et al. (eds) *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: Bloomsbury Collections, pp. 173–194.
Hackenesch C and Bader J (2020) The struggle for minds and influence: the Chinese Communist Party's global outreach. *International Studies Quarterly* 64(3): 723–733.
Hale E (2022) Taiwan government meme mocking China goes viral. *VOA News*, 1 April. Available at: https://www.voanews.com/a/taiwan-government-meme-mocking-china-goes-viral-/6510895.html
Harman G (2010) Technology, objects and things in Heidegger. *Cambridge Journal of Economics* 34(1): 17–25.
Hayden C (2012 [2011]) *The Rhetoric of Soft Power: Public Diplomacy in Global Contexts*. Lanham, MD: Rowman & Littlefield.
Hedling E and Ördén H (2025) Disinformation, deterrence and the politics of attribution. *International Affairs* 101(3): 967–986.
Heidegger M (2013) *The Question Concerning Technology and Other Essays*. New York: Harper Perennial.
Helmus T and Holynska K (2024) Ukrainian resistance to Russian disinformation; Lessons for future conflict. *RAND*, 3 September. Available at: https://www.rand.org/pubs/research_reports/RRA2771-1.html
Hille K (2021) Taiwan's unity cracks under Chinese disinformation onslaught. *Financial Times*, 28 June. Available at: https://www.ft.com/content/f22f1011-0630-462a-a21e-83bae4523da7

Hoijtink M and Leese M (2019) *Technology and Agency in International Relations*. Abingdon: Routledge.
Huang J-N (2023) China's propaganda and disinformation operations in Taiwan: a sharp power perspective. *China: An International Journal* 21(2): 143–170.
Hughes C (2015) Confucius institutes and the university: distinguishing the political mission from the cultural. *Issues and Studies* 50(4): 45–83.
Hung T-C and Hung T-W (2020) How China's cognitive warfare works: a frontline perspective of Taiwan's anti-disinformation wars. *Journal of Global Security Studies* 7(4): 1–18.
Jacobsen KL and Monsees L (2019) Co-production: the study of productive processes at the level of materiality and discourse. In: Hoijtink M and Leese M (eds) *Technology and Agency in International Relations*. Abingdon: Routledge, pp. 24–41.
Jasanoff S (2004) *States of Knowledge: The Co-Production of Science and the Social Order*. Abingdon: Routledge.
Jasanoff S (2005) *Designs on Nature: Science and Democracy in Europe and the United States*. Princeton, NJ: Princeton University Press.
Jasanoff S (2006) Technology as a site and object of politics. In: Tilly C and Goodin R (eds) *Oxford Handbook of Contextual Political Analysis*. Oxford: Oxford University Press, pp. 745–763.
Jasanoff S and Kim S-H (2009) Containing the atom: sociotechnical imaginaries and nuclear regulation in the U.S. and South Korea. *Minerva* 47(2): 119–146.
Jasanoff S and Kim S-H (2015) *Dreamscapes of Modernity*. Chicago, IL: University of Chicago Press.
Kao S-S (2021) Taiwan's response to disinformation a model for coordination to counter a complicated threat. *National Bureau of Asian Research*, 16 September. Available at: https://www.nbr.org/publication/taiwans-response-to-disinformation-a-model-for-coordination-to-counter-a-complicated-threat/
Karlova N and Fisher K (2013) A social diffusion model of misinformation and disinformation for understanding human information behaviour. *Information Research* 18(1).
Kaul N and Thornton M (2025) Construction and control of cartographic imaginaries: Kashmir and Taiwan. *Review of International Studies*. Epub ahead of print 4 April. DOI: 10.1017/S0260210525000129.
Kemp S (2023) Digital 2023: Taiwan. *Datareportal*, 13 February. Available at: https://datareportal.com/reports/digital-2023-taiwan
Kingsley P (2012) How tiny Estonia stepped out of USSR's shadow to become an internet titan. *Guardian*, 15 April. Available at: https://www.theguardian.com/technology/2012/apr/15/estonia-ussr-shadow-internet-titan
Kleinman DL and Moore K (2014) *Routledge Handbook of Science, Technology, and Society*. Abingdon: Routledge.
Kooiman J and Jentoft S (2009) Meta-governance: values, norms, and principles, and the making of hard choices. *Public Administration* 87(4): 818–836.
la Cour C (2020) Theorising digital disinformation in international relations. *International Politics* 57(4): 704–723.
Lahmann H (2022) Infecting the mind: establishing responsibility for transboundary disinformation. *European Journal of International Law* 33(2): 411–440.
Lambach D (2020) The territorialization of cyberspace. *International Studies Review* 22(3): 482–506.
Lange E and Lee D (2020) How one social media app is beating disinformation. *Foreign Policy*, 23 November. Available at: https://foreignpolicy.com/2020/11/23/line-taiwan-disinformation-social-media-public-private-united-states/

Lanoszka A (2019) Disinformation in international politics. *European Journal of International Security* 4(2): 227–248.
Latour B (1999) *Pandora's Hope: Essays on the Reality of Science Studies*. Cambridge, MA: Harvard University Press.
Lessenski M (2023) Finland tops the new media literacy index 2023, countries close to the war in Ukraine remain among the most vulnerable to disinformation. *Open Society Institute*, 24 June. Available at: https://osis.bg/?p=4450&lang=en (accessed 3 December 2024).
Lewandowsky S, Stritzke WGK, Freund AM, et al. (2013) Misinformation, disinformation, and violent conflict: from Iraq and the 'War on Terror' to future threats to peace. *American Psychologist* 68(7): 487–501.
Lien C-Y and Wu Y-H (2021) Affective communication: a mixed method investigation into COVID-19 outbreak communication using the Taiwanese government Facebook page. *Global Health Promotion* 28(2): 56–66.
Lien Y-T, Doowan L and Lange E (2021) Gamifying disinformation mitigation. *The Cipher Brief*, 15 July. Available at: https://www.thecipherbrief.com/column_article/gamifying-disinformation-mitigation
Lindquist J and Weltevrede E (2024) Authenticity governance and the market for social media engagements: the shaping of disinformation at the peripheries of platform ecosystems. *Social Media + Society* 10(1): 1–14.
LINE (2022) Digital Responsibility Program 數位當責計畫, 6 April. Available at: https://tinyurl.com/4dtdcu24
LINE FactChecker 訊息查證 (2023) 'Public Affairs', LINE FactChecker website. Available at: https://fact-checker.line.me/gov-announces (accessed 15 November 2023).
Lo P-C (2020) Cofacts, 27 April. Available at: https://en.cofacts.tw/search?type=replies&q=COVID (accessed 3 November 2023).
Lukes S (1974) *Power: A Radical View*. London: Macmillan.
Lupovici A (2023) Ontological security, cyber technology, and states' responses. *European Journal of International Relations* 29(1): 153–178.
Ma L and Van Brakel J (2014) Heidegger's thinking on the 'Same' of science and technology. *Continental Philosophy Review* 47(1): 19–43.
Maddox JD, Gentzel C and Levis A (2021) Toward a whole-of-society framework for countering disinformation. *Modern War Institute*, 10 May. Available at: https://mwi.westpoint.edu/toward-a-whole-of-society-framework-for-countering-disinformation/
Malmvig H (2023) Jesting international politics: the productive power and limitations of humorous practices in an age of entertainment politics. *Review of International Studies* 49(3): 513–534.
Manfredi J-L, Amado A and Gómez-Iniesta P (2022) State disinformation: emotions at the service of the cause. *Communication & Society* 35(2): 205–221.
Maschmeyer L (2021) The subversive trilemma: why cyber operations fall short of expectations. *International Security* 46(2): 51–90.
Maschmeyer L (2023) Subversion, cyber operations, and reverse structural power in world politics. *European Journal of International Relations* 29(1): 79–103.
Matei A and Irimia SI (2014) Open source governance – a more ambitious cousin of collaborative governance. *International Journal of Public Administration* 37(12): 812–823.
Matthewman S (2011) *Technology and Social Theory*. New York: Palgrave Macmillan.
Miller C (2019) Crossing divides: how a social network could save democracy from deadlock. *BBC News*, 26 October. Available at: https://www.bbc.co.uk/news/technology-50127713
Ministry of Defense of Ukraine (2022) X/Twitter, 27 November. Available at: https://tinyurl.com/563zn8aw (accessed 27 November 2023).

Ministry of Education 中華民國教育部 (2023) All-out defence education lesson video for elementary school for ages 3-6 教育部全民國防教育教學影片國民小學3-6年級學生版. Available at: https://www.youtube.com/watch?v=Pwpp0Ukw86A (accessed 9 October 2023).

Monsees L (2023) Information disorder, fake news and the future of democracy. *Globalizations* 20(1): 153–168.

NATO Parliamentary Assembly (2021) Resolution 466 – Developing a whole-of-society, integrated and coordinated approach to resilience for allied democracies. *Committee on Democracy and Security*, 11 October. Available at: https://www.nato-pa.int/document/resolution-466-developing-whole-society-integrated-and-coordinated-approach-resilience

Nielsen JH and Lindvall J (2021) Trust in government in Sweden and Denmark during the COVID-19 epidemic. *West European Politics* 44(5–6): 1180–1204.

Niinistö S (2024) Safer together: strengthening Europe's civilian and military preparedness and readiness. *European Commission*, 30 October. Available at: https://commission.europa.eu/document/5bb2881f-9e29-42f2-8b77-8739b19d047c_en

Nord L and Gardell E-KO (2023) Communicating the Covid-19 pandemic: a comparison of government communication in Denmark, Norway, and Sweden. In: Ihlen Ø, Johansson B, Lindholm J, et al. (eds) *Communicating a Pandemic: Crisis Management and Covid-19 in the Nordic Countries*. Gothenburg: Nordicom, University of Gothenburg, pp. 53–71.

OECD (2019) Chapter 13. Case Study 8: Estonia e-government and the creation of a comprehensive data infrastructure for public services and agriculture policies implementation. In: (N.a.) *Digital Opportunities for Better Agricultural Policies*. Paris: OECD Publishing, pp. 207–213. Available at: https://doi.org/10.1787/510a82b5-en

Papacharissi Z (2014) *Affective Publics: Sentiment, Technology, and Politics*. Oxford: Oxford University Press.

Pherson RH, Ranta PM and Cannon C (2021) Strategies for combating the scourge of digital disinformation. *International Journal of Intelligence and CounterIntelligence* 34(2): 316–341.

Pol.is (2024) *Polis Blog*. Available at: https://pol.is/home

Pollock A and Subramaniam B (2016) Introduction to special issue: resisting power, retooling justice: promises of feminist postcolonial technosciences. *Science, Technology, & Human Values* 41(6): 951–966.

Rawnsley M-Y (2016) Cultural democratisation and Taiwan cinema. In: Schubert G (ed.) *Routledge Handbook of Contemporary Taiwan*. London: Routledge, pp. 373–388.

Restivo S (2007 [1995]) The theory landscape in science studies: sociological traditions. In: Jasanoff S, Markle GE, Peterson JC, et al. (eds) *Handbook of Science and Technology Studies*. Thousand Oaks, CA: Sage, pp. 95–110.

Reus-Smit C (2007) International Crises of legitimacy. *International Politics* 44(2): 157–174.

Ruin H (2009) Ge-stell: enframing as the essence of technology. In: Davis B (ed.) *Martin Heidegger: Key Concepts*. Slough: Acumen Publishing, pp. 183–194.

Schattschneider E (1975) *The Semisovereign People: A Realist's View of Democracy in America*. Boston, MA: Cengage Learning.

Solomon T (2014) The affective underpinnings of soft power. *European Journal of International Relations* 20(3): 720–741.

Statista (2023) Market share of major instant messaging platforms in Taiwan as of May 2023. Available at: https://www.statista.com/statistics/968238/taiwan-communication-software-usage/

Taiwan AI Labs 台灣人工智慧實驗室 (2024) Taiwan presidential election information manipulation AI observation report, 31 January. Available at: https://ailabs.tw/wp-content/uploads/2024/01/2024-Taiwan-Presidential-Election-Information-Manipulation-AI-Observation-Report-2.pdf

Taiwan Ministry of Health and Welfare (2021) X/Twitter, 27 January. Available at: https://twitter.com/MOHW_Taiwan/status/1354333771198152708/photo/1 (accessed 2 April 2024).

Tang A 唐鳳 (2016) Uber responds to vTaiwan's coherent blended volition. *Polis Blog*, 23 May. Available at: https://blog.pol.is/uber-responds-to-vtaiwans-coherent-blended-volition-3e9b75102b9b (accessed 2 December 2021).

Tang A 唐鳳 (2017) 2017-10-29 MozFest. Public Digital Innovation Space (PDIS) Youtube Channel, 29 October. Available at: https://www.youtube.com/watch?v=bBcFnCenC4I (accessed 1 December 2021).

Templeman K (2020) How Taiwan Stands Up to China. *Journal of Democracy* 31(3): 85–99.

Tokariuk O (2023) Humour as a strategic tool against disinformation: Ukraine's response to Russia. *Reuters Institute*, June. Available at: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-12/RISJ%20Project_OlgaT_HT23_Final.pdf

Tuominen K and Savolainen R (1997) A social constructionist approach to the study of information use as discursive action. In: *Information Seeking in Context: Proceedings of the International Conference on Research in Information Needs, Seeking and Use in Different Contexts*, pp. 81–96.

TVBS Poll Center (2021) Survey of public approval of president Tsai Ing-wen and the COVID-19 pandemic 蔡英文總統滿意度與新冠肺炎疫情影響民調, 20 March. Available at: https://cc.tvbs.com.tw/portal/file/poll_center/2020/20200326/d1c2bea9ec4c-c133b96a8369f5115382.pdf

Ukrainian Ministry of Defence (2022) @DefenceU. *X/Twitter*. Available at: https://tinyurl.com/563zn8aw

Waisbord S (2018) Truth is what happens to news. *Journalism Studies* 19(13): 1866–1878.

Wang A, Lee M-C, Wu M-H, et al. (2020) Influencing overseas Chinese by tweets: text-images as the key tactic of Chinese propaganda. *Journal of Computational Social Science* 3(2): 469–486.

Wang T-L (2020) Does fake news matter to election outcomes? The case study of Taiwan's 2018 local elections. *Asian Journal for Public Opinion Research* 8(2): 67–104.

Wedeen L (1999) *Ambiguities of Domination: Politics, Rhetoric, and Symbols in Contemporary Syria*. Chicago, IL: University of Chicago Press.

Wigell M (2021) Democratic deterrence: how to dissuade hybrid interference. *The Washington Quarterly* 44(1): 49–67.

Wilner A (2024) Deterrence by de-legitimization in the information environment: concept, theory, and practice. In: Ouellet E, Stewart K and D'Agata M (eds) *Deterrence in the 21st Century: Statecraft in the Information Age*. Calgary, AB, Canada: University of Calgary Press, pp. 63–78.

Wohlforth WC (2020) Realism and great power subversion. *International Relations* 34(4): 459–481.

Wood J (2020) People in these countries think their government did a good job of dealing with the pandemic. *World Economic Forum*, 15 September. Available at: https://www.weforum.org/stories/2020/09/covid-19-survey-trust-unity-cooperation/

Yee A (2022) The country inoculating against disinformation. *BBC*, 31 January. Available at: https://www.bbc.com/future/article/20220128-the-country-inoculating-against-disinformation

Yeung K (2018) Algorithmic regulation: a critical interrogation. *Regulation & Governance* 12(4): 505–523.

Zhang C (2022) China's influence and the center-periphery Tug of War in Hong Kong, Taiwan and Indo-Pacific. *Democratization* 29(4): 773–775.

List of Interviews

Billion Lee, Co-facts founder and g0v member, 28 June 2023.
Former Member of the Participation Officer Network, 1 March 2024.
Open Culture Foundation 開放文化基金會 Personnel, 22 August 2023.

Author biography

Mariah Thornton is a doctoral candidate at the London School of Economics and Political Science (LSE) Department of International Relations and a researcher at LSE IDEAS. Her research focuses on China's foreign policy and strategy towards Taiwan, cross-Strait relations, and Taiwan in digital international relations. Before joining LSE, Mariah worked as a press and communications officer at the Taipei Representative Office in the United Kingdom for over two years. Mariah completed a BA in Chinese Studies at the University of Oxford (2011–2015) and an MSc in Chinese Politics at the School of Oriental and African Studies (2016–2017). She is the lead editor of *Taiwan's Economic and Diplomatic Challenges and Opportunities* (Routledge, 2021).